UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
16734 Crenshaw Boulevard
Torrance, California 90504

Case No. 2:18-MJ-02336

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachments A-1, A-2, and A-3

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-1, B-2, and B-3

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. §§ 841(a)(1), 843(b), 846, and 18 U.S.C. § 1956	Possession with Intent to Distribute Controlled Substances; Unlawful Use of a Communication Facility to Facilitate the Distribution of a Controlled Substance; Conspiracy and Attempt to Distribute Controlled Substances; and Money Laundering

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

DEA Special Agent Courtney L. Boeckman
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

_____
Judge's signature

City and state: Los Angeles, California

Honorable Steve Kim, U.S. Magistrate Judge
Printed name and title

AUSA: Catherine S. Ahn, x2424

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

The property to be searched is 16734 Crenshaw Boulevard, Torrance, California 90504 (the "SUBJECT PREMISES"), as well as any safes, safe deposit boxes, garages, attached or detached structures located at the premises, vehicles associated with REGALADO in the driveway, garage, or located at or near the SUBJECT PREMISES.

The SUBJECT PREMISES is located within a multi-family, two-story residence comprised of a brown stucco-style construction, with dark brown trim. The numbers "16732" are posted on the front of the building, which identifies the building itself, but not the SUBJECT PREMISES. The front door of the SUBJECT PREMISES bears the numbers "34," identifying the precise address of the SUBJECT PREMISES – 16734 Crenshaw Boulevard. The front door of the SUBJECT PREMISES is located in the main entrance alcove on the ground level of the building. The SUBJECT PREMISES also includes an apparent detached or disconnected garage, which displays the numbers "34" above the garage door.

ATTACHMENT A-2

VEHICLE TO BE SEARCHED

The vehicle to be searched is a brown- or gold-colored 2015 Nissan Altima bearing Vehicle Identification Number 1N4AL3AP4FC293620 and California license plate number 7XJL306 (the "SUBJECT VEHICLE").

ATTACHMENT A-3

PERSON TO BE SEARCHED

The person of Meagan GONZALEZ ("GONZALEZ"), date of birth November 14, 1983 with California Driver's License Number B8486230. GONZALEZ's California Department of Motor Vehicle records lists her as being five feet and seven inches tall, weighing approximately 180 pounds, and having brown eyes and brown hair.

The search of GONZALEZ shall include any and all clothing and personal belongings, digital devices, backpacks, wallets, briefcases, purses, and bags that are within GONZALEZ's immediate vicinity and control at the location where the search warrant is executed. The search of GONZALEZ shall not include a strip search or a body cavity search.

ATTACHMENT B-1

I. ITEMS TO BE SEIZED

1. The items to be seized are fruits, instrumentalities, and evidence of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. §§ 843(b) (Unlawful Use of a Communication Facility to Facilitate the Distribution of a Controlled Substance) 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), and 18 U.S.C. § 1956 (money laundering) (collectively, the "SUBJECT OFFENSES"), namely:

a. Any firearms, ammunition, silencers, explosives, incendiary devices, and other dangerous weapons;

b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing and canning devices, balloons, packaging materials, aromatic substances such as laundry soap, dryer sheets, air fresheners, or axle grease, containers, and money counters;

c. Items used in the packaging of currency for consolidation and transportation, including money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

d. Documents, records, and other items relating to the use of USPS or commercial express mail delivery companies, such as FedEx and UPS, to ship drugs and money to various points

within the United States, including air bills, empty or previously used mailing boxes, packing tape, packaging materials, package tracking records, and transaction receipts;

e. Documents and records relating to travel by air, bus, car, or other means, including calendars, travel itineraries, maps, airline ticket, baggage check stubs, frequent use club membership information, airline, hotel and rental car receipts, credit card bills and receipts, photographs, videos, passports, and visas;

f. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply for controlled substances, or drug customers, sources of funds, financial records, records that may indicate ownership of cash and funds, including calendars, address books, telephone or other contact lists, hard copy correspondence, notes, photographs, and videos;

g. Records, documents, programs, applications or materials relating to the trafficking of controlled substances, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and times when controlled substances were bought, sold, or otherwise distributed;

h. Documents and keys relating to public storage units, rental cars, safety deposit boxes, or Commercial Mail Receiving Agencies;

i. Any shipping materials related to the SUBJECT OFFENSES, including, but not limited to: envelopes, boxes, and containers;

j. Any mail packages used to facilitate the SUBJECT OFFENSES, whether opened or unopened, believed to be in the possession, dominion, or control of REGALADO or his criminal co-conspirators;

k. Records showing ownership, dominion, or control over the SUBJECT PREMISES, including utility statements and records, journals, records of occupancy, rental or lease agreements, letters, notes, and correspondence.

l. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of drugs, or drug customers, including calendars, address books, telephone or other contact lists, hard copy correspondence, and notes;

m. United States currency over $2,000 or bearer instruments worth over $2,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first $2,000);

n. Records, documents, programs, applications, or materials reflecting or relating to payment, receipt, concealment, transfer, or movement of money, including but not limited to bank account records and other financial institution records, wire transfer records, receipts, safe deposit box keys and records, and notes; and

o. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

p. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

q. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

r. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

s. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

t. Contents of any calendar or date book;

u. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

v. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

2. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters,

monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

5. In searching the digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any digital device capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each digital device where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of a digital device as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search a digital device beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the digital device and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that digital device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return

the digital device and delete or destroy all forensic copies thereof.

g. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of a digital device, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. During the execution of this search warrant, law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of Andres REGALADO and Meagan GONZALEZ onto

the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of Andres REGALADO and Meagan GONZALEZ face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT B-2

I. ITEMS TO BE SEIZED

1. The items to be seized are fruits, instrumentalities, and evidence of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. §§ 843(b) (Unlawful Use of a Communication Facility to Facilitate the Distribution of a Controlled Substance) 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), and 18 U.S.C. § 1956 (money laundering) (collectively, the "SUBJECT OFFENSES"), namely:

a. Any firearms, ammunition, silencers, explosives, incendiary devices, and other dangerous weapons;

b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing and canning devices, balloons, packaging materials, aromatic substances such as laundry soap, dryer sheets, air fresheners, or axle grease, containers, and money counters;

c. Items used in the packaging of currency for consolidation and transportation, including money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

d. Documents, records, and other items relating to the use of USPS or commercial express mail delivery companies, such as FedEx and UPS, to ship drugs and money to various points

within the United States, including air bills, empty or previously used mailing boxes, packing tape, packaging materials, package tracking records, and transaction receipts;

e. Documents and records relating to travel by air, bus, car, or other means, including calendars, travel itineraries, maps, airline ticket, baggage check stubs, frequent use club membership information, airline, hotel and rental car receipts, credit card bills and receipts, photographs, videos, passports, and visas;

f. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply for controlled substances, or drug customers, sources of funds, financial records, records that may indicate ownership of cash and funds, including calendars, address books, telephone or other contact lists, hard copy correspondence, notes, photographs, and videos;

g. Records, documents, programs, applications or materials relating to the trafficking of controlled substances, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and times when controlled substances were bought, sold, or otherwise distributed;

h. Documents and keys relating to public storage units, rental cars, safety deposit boxes, or Commercial Mail Receiving Agencies;

i. Any shipping materials related to the SUBJECT OFFENSES, including, but not limited to: envelopes, boxes, and containers;

j. Any mail packages used to facilitate the SUBJECT OFFENSES, whether opened or unopened, believed to be in the possession, dominion, or control of REGALADO or his criminal co-conspirators;

k. Records showing ownership, dominion, or control over the SUBJECT VEHICLE, including car registration documents, insurance documents, and car transfer documents.

l. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of drugs, or drug customers, including calendars, address books, telephone or other contact lists, hard copy correspondence, and notes;

m. United States currency over $2,000 or bearer instruments worth over $2,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first $2,000);

n. Records, documents, programs, applications, or materials reflecting or relating to payment, receipt, concealment, transfer, or movement of money, including but not limited to bank account records and other financial institution records, wire transfer records, receipts, safe deposit box keys and records, and notes; and

o. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

p. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

q. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

r. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

s. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

t. Contents of any calendar or date book;

u. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

v. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

2. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters,

monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR SUBJECT VEHICLE

5. In searching the SUBJECT VEHICLE, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will search the SUBJECT VEHICLE where it is currently located, or may, at its discretion, transport the vehicle to an appropriate law enforcement facility to be searched at that location.

b. In searching the SUBJECT VEHICLE for a hidden compartment, law enforcement will initially attempt to find the hidden compartment using visual methods. However, at the search team's discretion, the search team may remove portions of the SUBJECT VEHICLE to conduct a more thorough search. The search team will re-assemble or re-attach any removed portions of the SUBJECT VEHICLE.

III. SEARCH PROCEDURE FOR DIGITAL DEVICES

6. In searching the digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

c. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any digital device capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

d. The search team will, in its discretion, either search each digital device where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

e. The search team shall complete the search of a digital device as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search a digital device beyond this 120-day period without obtaining an extension of time order from the Court.

f. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the digital device and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

g. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that digital device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

h. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the digital device and delete or destroy all forensic copies thereof.

i. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

j. If the search determines that the digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the

government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

k. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

l. After the completion of the search of a digital device, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

7. During the execution of this search warrant, law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of Andres REGALADO and Meagan GONZALEZ onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of Andres REGALADO and Meagan GONZALEZ face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

8. The special procedures relating to digital devices found in this warrant govern only the search of digital devices

pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

ATTACHMENT B-3

I. ITEMS TO BE SEIZED

1. The items to be seized are fruits, instrumentalities, and evidence of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. §§ 843(b) (Unlawful Use of a Communication Facility to Facilitate the Distribution of a Controlled Substance) 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), and 18 U.S.C. § 1956 (money laundering) (collectively, the "SUBJECT OFFENSES"), namely:

a. Any firearms, ammunition, silencers, explosives, incendiary devices, and other dangerous weapons;

b. Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing and canning devices, balloons, packaging materials, aromatic substances such as laundry soap, dryer sheets, air fresheners, or axle grease, containers, and money counters;

c. Items used in the packaging of currency for consolidation and transportation, including money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;

d. Documents, records, and other items relating to the use of USPS or commercial express mail delivery companies, such as FedEx and UPS, to ship drugs and money to various points

within the United States, including air bills, empty or previously used mailing boxes, packing tape, packaging materials, package tracking records, and transaction receipts;

e. Documents and records relating to travel by air, bus, car, or other means, including calendars, travel itineraries, maps, airline ticket, baggage check stubs, frequent use club membership information, airline, hotel and rental car receipts, credit card bills and receipts, photographs, videos, passports, and visas;

f. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply for controlled substances, or drug customers, sources of funds, financial records, records that may indicate ownership of cash and funds, including calendars, address books, telephone or other contact lists, hard copy correspondence, notes, photographs, and videos;

g. Records, documents, programs, applications or materials relating to the trafficking of controlled substances, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and times when controlled substances were bought, sold, or otherwise distributed;

h. Documents and keys relating to public storage units, rental cars, safety deposit boxes, or Commercial Mail Receiving Agencies;

i. Any shipping materials related to the SUBJECT OFFENSES, including, but not limited to: envelopes, boxes, and containers;

j. Any mail packages used to facilitate the SUBJECT OFFENSES, whether opened or unopened, believed to be in the possession, dominion, or control of REGALADO or his criminal co-conspirators;

k. Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of drugs, or drug customers, including calendars, address books, telephone or other contact lists, hard copy correspondence, and notes;

l. United States currency over $2,000 or bearer instruments worth over $2,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first $2,000);

m. Records, documents, programs, applications, or materials reflecting or relating to payment, receipt, concealment, transfer, or movement of money, including but not limited to bank account records and other financial institution records, wire transfer records, receipts, safe deposit box keys and records, and notes; and

n. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers

accessed through any push-to-talk functions, as well as all received or missed incoming calls;

o. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

p. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

q. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

r. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

s. Contents of any calendar or date book;

t. Global Positioning System (“GPS”) coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

u. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

2. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

a. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

b. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment of other devices;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

e. evidence of the times the device was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the device;

g. applications, utility programs, compilers, interpreters, or other software, as well as documentation and

manuals, that may be necessary to access the device or to conduct a forensic examination of it;

h. records of or information about Internet Protocol addresses used by the device;

i. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

3. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

4. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to

store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

5. In searching the digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any digital device capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each digital device where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of a digital device as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search a digital device beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the digital device and any data thereon falls within the

scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that digital device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the digital device and delete or destroy all forensic copies thereof.

g. If the search determines that a digital device does contain data falling within the list of items to be seized,

the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of a digital device, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

6. During the execution of this search warrant, law enforcement personnel are authorized to: (1) depress the thumb- and/or fingerprints of Andres REGALADO and Meagan GONZALEZ onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the face of Andres REGALADO and Meagan GONZALEZ face with his or

her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

7. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Courtney L. Boeckman, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search 16734 Crenshaw Boulevard, Torrance, California 90504 (the "SUBJECT PREMISES"), as described more fully in Attachment A-1, a sedan with California license plate 7XJL306 either brown or gold in color (the "SUBJECT VEHICLE"), as described more fully in Attachment A-2, and the person of Meagan GONZALEZ ("GONZALEZ"), as described more fully in Attachment A-3. The requested search warrant seeks authorization to seize evidence, fruits, and instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 21 U.S.C. §§ 843(b) (Unlawful Use of a Communication Facility to Facilitate the Distribution of a Controlled Substance) 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances), and 18 U.S.C. § 1956 (money laundering) (collectively, the "SUBJECT OFFENSES"), as described more fully in Attachment B-1, B-2, and B-3. Attachments A-1, A-2, A-3, and B-1, B-2, and B-3 are incorporated herein by reference.

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant,

and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

3. I am a Special Agent with the United States Drug Enforcement Administration ("DEA") and have been so employed since February 2015. I am currently assigned to DEA's Los Angeles Field Division, High Intensity Drug Trafficking Area ("HIDTA") Group 46. During my career as a Special Agent with DEA, I have received training and experience in interviewing and interrogation techniques, arrest procedures, search and seizure, narcotics investigations, search warrant applications, and various other crimes. In the course of my training and experience, I have become familiar with the methods and techniques associated with the distribution of narcotics, the laundering of drug proceeds, and the organization of drug conspiracies. Through instruction and participation in investigations, I have become familiar with the manner in which narcotics traffickers conduct their illegal business and the methods, language, and terms that are used to disguise conversations about their narcotics activities. I have also become familiar with the methods and techniques associated with the distribution of narcotics, the laundering of drug proceeds, and the organization of drug conspiracies.

III. SUMMARY OF PROBABLE CAUSE

4. Andres REGALADO ("REGALADO"), also known as "Andy," was identified by cooperating defendants Maurice BROWN[1] and Linnel GRAHAM[2] ("GRAHAM") as a source of supply for methamphetamine that BROWN was mailing from the Los Angeles metropolitan area to recipients in Memphis, Tennessee, including GRAHAM. BROWN identified a telephone number ending in 4568 as one of REGALADO's telephone numbers (the "4568 phone number"), and stated that he had directed individuals in Tennessee to use bank accounts for GONZALEZ to pay REGALADO for drugs. GRAHAM and BROWN both identified GONZALEZ as REGALADO's girlfriend. Telephone records for the 4568 phone number show that the subscriber for this number, which was used by BROWN to contact REGALADO for drugs, is GONZALEZ. GONZALEZ was also identified by BROWN and GRAHAM as being present at REGALADO's previous residence when they were there to purchase drugs.

5. BROWN further identified a brown sedan with California license plate 7XJL306 (the SUBJECT VEHICLE) as used by REGALADO, and that it contains a hidden compartment used by REGALADO to

---

[1] BROWN is under federal indictment for his role in this conspiracy. He is cooperating in exchange for judicial consideration. Investigators have deemed BROWN to be reliable. In addition to his prior drug convictions, BROWN has a 2004 misdemeanor for passing a bad check in violation of California Penal Code Section 475(c).

[2] GRAHAM was charged by state authorities for drug offenses and cooperated in exchange for judicial consideration. He is currently under federal indictment and is continuing to cooperate in exchange for judicial consideration. Investigators have deemed GRAHAM to be reliable, and, among other convictions, has a prior fraud conviction for counterfeiting United States currency in violation of 18 U.S.C. § 472 in 2000.

store, transport, and hide drugs. The SUBJECT VEHICLE is registered to both REGALADO and GONZALEZ and law enforcement has seen it parked at the SUBJECT PREMISES. REGALADO currently lives at the SUBJECT PREMISES.

IV. STATEMENT OF PROBABLE CAUSE

A. Background of the Conspiracy and the Investigation

6. Since approximately March of 2017, DEA and the United States Postal Inspection Service ("USPIS") have been investigating an interstate criminal organization responsible for trafficking multi-pound quantities of methamphetamine from the Los Angeles metropolitan area in California to the City of Memphis, Tennessee and the surrounding region.

7. Law enforcement intercepted two packages on or about March 16, 2017 and a third package on or about July 8, 2017, containing approximately one half-pound of methamphetamine each. The methamphetamine was lab-tested and confirmed to be 99% pure methamphetamine. The packages were sent through the United States Postal Service from California to addresses in Tennessee, including an address that law enforcement identified as belonging to Alyson PAYNE ("PAYNE") through law enforcement databases. In July 2018, law enforcement did a controlled delivery of the third package, which was addressed to PAYNE, and arrested GRAHAM when GRAHAM went to pick up the package from the residential building's office. GRAHAM identified himself as PAYNE's boyfriend to law enforcement following his arrest.

8. Postal surveillance video showed an individual shipping each of the above-described packages. By looking at

GRAHAM's public social media pages, law enforcement were able to recognize an individual in one of the photographs as the same individual seen in the postal surveillance video. GRAHAM identified the individual as BROWN, who resides in California.

9. A review of postal records revealed that from approximately late 2016 to August 2017, BROWN and suspected co-conspirators had repeatedly shipped parcels to addresses in Tennessee, including addresses identified as belonging to GRAHAM and PAYNE through surveillance and law enforcement databases. In addition to seizing methamphetamine shipped by BROWN to Tennessee, law enforcement also successfully seized shipments of illegally diverted pharmaceutical opioids and marijuana. During the course of a controlled delivery operation, law enforcement also seized drug proceeds.

10. On February 13, 2018, a federal Grand Jury in the Western District of Tennessee returned an indictment charging BROWN, GRAHAM, PAYNE, and other co-conspirators with violations of 21 U.S.C. §§ 841, 846 and 18 U.S.C. § 2. On February 15, 2018, BROWN, GRAHAM, PAYNE and other indicted co-defendants were taken into federal custody.

B. BROWN Identifies "Andy" as His Source of Methamphetamine Supply and the SUBJECT VEHICLE

11. Following his arrest, BROWN began providing information about his source of methamphetamine supply through proffer interviews.

12. BROWN stated that he shipped parcels containing large quantities of prescription pills to GRAHAM and another co-

defendant, but began to ship methamphetamine after being asked if BROWN had access to the drug. BROWN successfully began to obtain methamphetamine from an individual that he knew as "Andy" (later identified by law enforcement as REGALADO) in packages physically packaged by REGALADO. After a series of shipments, BROWN began to purchase pound-quantities of crystal methamphetamine from REGALADO for $3,200 per pound. BROWN would receive the methamphetamine at REGALADO's residence, which at the time was on Lennox Blvd in Inglewood, California (the "Lennox Boulevard address").[3]

13. After receiving the methamphetamine from REGALADO, BROWN said that he would store the methamphetamine at BROWN's residence, where BROWN would divide the drugs into smaller quantities for subsequent interstate distribution. In return, GRAHAM and another co-defendant would fly to California with drug proceeds to purchase more methamphetamine. Further, GRAHAM and the other co-defendant would also ship parcels of drug proceeds (in bulk United States currency) to BROWN's residence in Los Angeles. Finally, BROWN gave his Memphis-based co-conspirators the banking information for an individual BROWN believed was REGALADO's girlfriend (later identified as Meagan GONZALEZ, as further described below), so that the Memphis

[3] The Los Angeles, California Office of the DEA previously investigated REGALADO's activities from 2013-2016. This investigation resulted in the seizure of a multi-kilogram quantity of cocaine and a multi-pound quantity of methamphetamine that was coordinated by REGALADO. During the course of the undercover investigation targeting REGALADO, REGALADO informed an undercover DEA Special Agent that he preferred to conduct narcotics transactions at his own residence, consistent with his dealings with BROWN.

conspirators could pay REGALADO for drugs through bank deposits. BROWN stated that he had previously seen REGALADO's girlfriend at REGALADO's house.

14. BROWN stated that he was paid at least $15,000 from methamphetamine sales over the course of the multi-year conspiracy. BROWN also stated REGALADO would deliver the methamphetamine to him in a brown sedan. BROWN said he believed the sedan had a hidden compartment based on discussion BROWN had with REGALADO, and that the hidden compartment is used to transport and hide drugs. BROWN did not know where the hidden compartment was located in the car.

15. Furthermore, BROWN stated that on or about April 19, 2018, REGALADO came to BROWN's house unannounced to ask BROWN for money owed to REGALADO for methamphetamine. REGALADO had provided BROWN two pounds of methamphetamine, worth $6,000, without asking for prior payment. However, the methamphetamine had been seized by law enforcement in Memphis. BROWN believed REGALADO owed another individual money for the methamphetamine REGALADO had provided to BROWN. After BROWN told REGALADO that BROWN had been arrested on federal charges in Memphis, however, REGALADO no longer appeared interested in the debt, and BROWN has not heard from REGALADO since that conversation.

16. BROWN further told law enforcement that he knows REGALADO to possess a 9mm pistol, which REGALADO kept in his house next to his chair. BROWN said that REGALADO, drove a brown car, possibly a Honda, with a California license plate number of 7XJL306 (later identified as the SUBJECT VEHICLE, as

described below). BROWN wrote down the license plate number after REGALADO visited him on April 19, 2018 to collect money.

C. Law Enforcement and BROWN Identify "Andy" as REGALADO

17. California DMV records for the license plate number provided by BROWN show that it belongs to a 2015 Nissan Altima (the SUBJECT VEHICLE) registered to REGALADO and GONZALEZ, at an apartment located at the Lennox Boulevard address. This is the same location that BROWN identified as being REGALADO's residence, and where BROWN would get methamphetamine from REGALADO.

18. A criminal history check for REGALADO shows an extensive criminal history that includes multiple drug, firearms, and violent offenses, including robbery, firearms possession, and spousal battery. He is also documented as a suspected gang member.

19. DEA created an official DEA photographic line-up, which included a photograph of Andres REGALADO obtained through law enforcement databases. BROWN positively identified the photograph of REGALADO as "Andy," his source of methamphetamine supply. Similarly, GRAHAM – who, according to BROWN, had taken GRAHAM to REGALADO's house to purchase drugs – identified a photograph of REGALADO as BROWN's source of supply.

20. During the course of a proffer interview, BROWN provided the 4568 phone number as one of the phone numbers he used to contact REGALADO. Investigators subsequently obtained subscriber information for this telephone number through administrative subpoenas and found that it was subscribed to

GONZALEZ at an address on W. 106th Street in Inglewood, California.

21. During a proffer interview in late August 2018, BROWN was shown the California DMV photograph of GONZALEZ and positively identified her as REGALADO's girlfriend, whose bank accounts BROWN had provided to Memphis co-conspirators in order to send money for drugs back to REGALADO.

22. On July 5, 2018, the Honorable Tu M. Pham, United States Magistrate Judge for the Western District of Tennessee, authorized the search and seizure of historical cell site records and other information to and from the 4568 phone number. A subsequent review of this data by DEA investigators revealed that the user of this telephone, suspected to be REGALADO, was in the same sector of Los Angeles County as BROWN was located in the 24 hours prior to each of the interdicted methamphetamine shipments, consistent with BROWN's information that he was picking up the drugs from REGALADO for shipment to Tennessee.

23. Investigators served CarMax with an administrative subpoena about REGALADO, GONZALEZ, and the SUBJECT VEHICLE. The responsive documents identified the SUBJECT VEHICLE as "gold" in color, and included REGALADO's full name and his California driver's license number. In addition, next to REGALADO's signature, REGALADO listed his telephone number as the same 4568 phone number provided by BROWN.

D. Law Enforcement Identify the SUBJECT PREMISES as REGALADO's Current Residence

24. Since BROWN had told REGALADO that he had been arrested, law enforcement conducted searches on open-source and government databases to find REGALADO's current address. I know, based on training and experience, that drug traffickers often store drugs and conduct drug transactions at their residence, and will often change residences in order to maintain operational security after a co-conspirator has been arrested.

25. Database search results and surveillance show that REGALADO's residence is currently listed as 16734 Crenshaw Boulevard, Torrance, California 90504 (the "SUBJECT PREMISES"). For example, REGALADO's DMV records list the SUBJECT PREMISES as REGALADO's sole address. Furthermore, law enforcement surveillance conducted throughout July and August of 2018 show that REGALADO is using the SUBJECT PREMISES as his residence. On or about July 10, 2018, investigators saw REGALADO at the SUBJECT PREMISES, and further saw REGALADO at the SUBJECT PREMISES in the same SUBJECT VEHICLE previously identified by BROWN as being driven by REGALADO. Law enforcement repeatedly saw the SUBJECT VEHICLE at the SUBJECT PREMISES throughout July and August 2018. In addition, on or about August 23, 2018, investigators again saw REGALADO at the SUBJECT PREMISES.

26. On August 23, 2018, the Honorable Diane K. Vescovo, United States Magistrate Judge for the Western District of Tennessee, authorized a search and seizure warrant for geo-location information associated with the 4568 phone number

believed to be used by REGALADO. Consistent with law enforcement's physical surveillance of the SUBJECT PREMISES, the results of the geo-location warrant provided over the past week have shown that the telephone is frequently located at or near the SUBJECT PREMISES. Furthermore, for the time the geo-location information has been received for the 4568 phone number, it has not been shown at the Lennox Boulevard address.

27. Based on the information described above, I believe the SUBJECT PREMISES will contain evidence related to the SUBJECT OFFENSES, and that REGALADO is currently using the SUBJECT PREMISES as his residence.

V. TRAINING AND EXPERIENCE RELATED DRUG SMUGGLING OFFENSES

28. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often use other individuals, including their girlfriends and spouses, to facilitate their drug trafficking offenses. For example, they often use girlfriends or spouses to hold digital devices or drugs on their

behalf, use the girlfriend or spouse to hold, send, or receive assets so that the assets cannot be traced back to the trafficker by law enforcement, and ask them to destroy items after arrest or a law enforcement encounter so that it will not be subject to search and seizure.

c. In addition, it is common for drug traffickers to create hidden compartments in their cars in order to store drugs and hide them from law enforcement while transporting the drugs. These compartments can range in quality from crude to highly sophisticated, including compartments that are designed to evade detection by scanners and other forms of visual and machine-based inspection. The more sophisticated compartments can take significant time and resources to detect, and may be placed in such a manner that a significant portion of the car may need to be dismantled in order to access the compartment.

d. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where the drug trafficker has ready access to them, such as on their cell phones and other digital devices.

e. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion

of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

f. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

g. Individuals engaged in the illegal purchase or sale of drugs and other contraband often use multiple digital devices.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

29. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and

connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

30. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that it is not always possible to search digital devices for digital data in a single day or even over several weeks for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it takes time to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, operating system, and software application being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the SUBJECT PREMISES. Storage devices capable of storing 500 or more gigabytes are now commonplace. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet.[4] Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or

[4] These statements do not generally apply to data stored in volatile memory such as random-access memory, or "RAM," which data is, generally speaking, deleted once a device is turned off.

recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has

been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the

absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

g. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime. In addition, decryption of devices and data stored thereon is a constantly evolving field, and law enforcement agencies continuously develop or acquire new methods of decryption, even for devices or data that cannot currently be decrypted.

31. As discussed herein, based on my training and experience I believe that digital devices enabled with biometric unlock functionality will be found during the search of the SUBJECT PREMISES, the SUBJECT VEHICLE, and of GONZALEZ.

a. I know from my training and experience and my review of publicly available materials that several hardware and software manufacturers offer their users the ability to unlock their devices through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint-recognition, face-recognition, iris-recognition, and retina-recognition. Some devices offer a combination of these biometric features and enable the users of such devices to select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple Inc. ("Apple") offers a feature on some of its phones and laptops called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which on a cell phone is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the phone, and on a laptop is located on the right side of the "Touch Bar" located directly above the keyboard. Fingerprint-recognition features are increasingly common on modern digital

devices. For example, for Apple products, all iPhone 5S to iPhone 8 models, as well as iPads (5th generation or later), iPad Pro, iPad Air 2, and iPad mini 3 or later, and MacBook Pro laptops with the Touch Bar are all equipped with Touch ID. Motorola, HTC, LG, and Samsung, among other companies, also produce phones with fingerprint sensors to enable biometric unlock by fingerprint. The fingerprint sensors for these companies have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. To activate the facial-recognition feature, a user must hold the device in front of his or her face. The device's camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the camera detects a face with characteristics that match those of the registered face. No physical contact by the user with the digital device is necessary for the unlock, but eye contact with the camera is often essential to the proper functioning of these facial-recognition features; thus, a user must have his or her eyes open during the biometric scan (unless the user previously disabled this requirement). Several companies produce digital devices equipped with a facial-recognition-unlock feature, and all work in a similar manner with different degrees of sophistication, e.g., Samsung's Galaxy S8 (released Spring 2017) and Note8 (released Fall 2017), Apple's iPhone X (released

Fall 2017). Apple calls its facial-recognition unlock feature "Face ID." The scan and unlock process for Face ID is almost instantaneous, occurring in approximately one second.

d. While not as prolific on digital devices as fingerprint- and facial-recognition features, both iris- and retina-scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable. Iris-recognition technology uses mathematical pattern-recognition techniques to map the iris using infrared light. Similarly, retina scanning casts infrared light into a person's eye to map the unique variations of a person's retinal blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate the feature, the user holds the device in front of his or her face while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data from the person's eyes. The device is then unlocked if the camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris-recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features including fingerprint-, facial-, and iris-unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, e.g., attachable infrared cameras or fingerprint sensors, to enable the Windows Hello features on older devices.

32. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

33. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features have been enabled. This can occur when a device has been restarted or inactive, or has not been unlocked for a certain period of time. For example, with Apple's biometric unlock features, these circumstances include when: (1) more than 48 hours has passed since the last time the device was unlocked; (2) the device has not been unlocked via Touch ID or Face ID in eight hours and the passcode or password has not been entered in the last six days; (3) the device has been turned off or restarted; (4) the device has received a remote lock command; (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made; or (6) the user has activated "SOS" mode by rapidly clicking the right side button five times or pressing and holding both the side button and either volume button. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric

features, the opportunity to unlock the device through a biometric feature may exist for only a short time. I do not know the passcodes of the devices likely to be found during the search.

34. For these reasons, if while executing the warrant, law enforcement personnel encounter a digital device that may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to: (1) compel the use of REGALADO and GONZALEZ's thumb- and/or fingerprints on the devices; and (2) hold the devices in front of REGALADO and GONZALEZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature. With respect to fingerprint sensor-enabled devices, although I do not know which of the fingers are authorized to access any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors; and, in any event, all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

35. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. REQUEST FOR NIGHTTIME SERVICE

36. I request that the Court authorize investigators to serve these warrants during the nighttime, as set forth under Fed. R. Crim. Proc. 41(e)(2)(A)(ii). Good cause for such service exists because, as discussed herein, REGALADO is

believed to be armed and has been prosecuted for multiple drug, firearms, and violent offenses. He is also documented to be a suspected gang member. If law enforcement were to execute these warrants during the daytime, it would be difficult to evade detection and would, thus, pose a risk for officer safety. Because GONZALEZ, as REGALADO's girlfriend, and the SUBJECT VEHICLE, which is REGALADO'S car, are both likely to be at the SUBJECT PREMISES, I am requesting night service as to the premises described in Attachments A-1, A-2, and A-3.

37. Given the holding set forth in Gooding v. United States, 416 U.S. 430 (1974), that there is no need for the presence of exigent circumstances in narcotics cases to justify a nighttime search, I believe that nighttime service is warranted in this case.

VIII. REQUEST FOR NO-KNOCK AUTHORIZATION

38. Based on my background, training, experience, and knowledge of this investigation, I have reasonable suspicion to believe that knocking and announcing law enforcement's presence at the SUBJECT PREMISES prior to executing the warrant would be dangerous and would inhibit the effective investigation of the SUBJECT OFFENSES by allowing for the destruction of evidence.[5]

[5] See Richards v. Wisconsin, 520 U.S. 385, 395 (1997) ("In order to justify a 'no-knock' entry, the police must have a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence. This standard-as opposed to a probable-cause requirement-strikes the appropriate balance between the legitimate law enforcement concerns at issue in the execution of search warrants and the individual privacy interests affected by no-knock entries.")

39. As described above, REGALADO is known to possess firearms and has taken steps to create hiding locations for his drugs. REGALADO also has a history of violent offenses, to include robbery, arrests for assault, and probation violations related to battery. To the extent REGALADO is present during the execution of the warrants at the SUBJECT PREMISES that is believed to be his home, it is certainly possible that these individuals will be armed with firearms and other weapons. Because GONZALEZ, as REGALADO's girlfriend, and the SUBJECT VEHICLE, which is REGALADO'S car, are both likely to be at the SUBJECT PREMISES, I am requesting that law enforcement not be required to knock and announce as to the premises described in Attachments A-1, A-2, and A-3.

40. Based on the evidence described above, I believe that knocking and announcing entry would be dangerous to the law enforcement personnel serving the warrant, given the high likelihood that firearms will be present at the SUBJECT PREMISES. Knocking and announcing would also allow for the quick destruction or transfer of evidence, namely narcotics, ledgers, money, and firearms.

IX. CONCLUSION

41. For all of the reasons described above, there is probable cause to believe that the items to be seized described in Attachments B-1, B-2, and B-3 will be found in a search of, respectively, the SUBJECT PREMISES described in Attachment A-1, the SUBJECT VEHICLE described in Attachment A-2, and of the person described in Attachment A-3.

Courtney L. Boeckman,
Special Agent, Drug Enforcement Administration

Subscribed to and sworn before me this ___ day of August, 2018.

THE HONORABLE STEVE KIM
UNITED STATES MAGISTRATE JUDGE